American
FIBER SYSTEMS

100 Meridian Centre
Suite 250
Rochester, NY 14618-3979

Director - Regulatory Affairs & Contract Management
Phone: (585) 340-5400, x150
Fax: (585) 340-5401
mnighan@americanfibersystems.com

February 29, 2008
Via Overnight Carrier

Federal Communications Commission
Enforcement Bureau
445 12th. Street SW
Room 7-C723
Washington, DC 20554

Re: CY 2007 Annual CPNI Certification
EB Docket No. 06-36

Dear Sir/Madam:

As required by 47 C.F.R.§64.2009(e) **American Fiber Systems, Inc.** hereby submits one (1) original of its annual CPNI compliance certification for Calendar Year 2007.

Sincerely,

Michael J. Nighan
Director - Regulatory Affairs & Contract Management

Enclosure

AMERICAN FIBER SYSTEMS, INC.

CY 2007 Annual Statement of CPNI Operating Procedures

Compliance with 47 C.F.R. Section 64.2005 through Section 64.2011

1. During CY 2007 American Fiber Systems, Inc. ("AFS") offered and provided High Capacity Competitive Local Exchange Carrier telecommunications services, such services falling into the "local" category of service. AFS marketed and provided such service exclusively to Enterprise and Carrier customers and did not market or provided service to residential customers.

2. Although holding a Global Resale International Telecommunications Certificate from the Commission, AFS did not market any form of international service to existing or new customers. Nor did AFS market any form of interexchange service to existing or new customers.

3. Neither has AFS ever marketed or provided any form of Commercial Mobile Radio Service to new or existing customers.

4. Accordingly, CPNI was used by AFS exclusively to market and provide services within the "local" category and AFS did not disclose or permit access to CPNI for the marketing or provision of services outside of the "local" category.

5. Therefore, new or existing AFS customers did not have the ability to subscribe with AFS for services within either the "interexchange" or "CMRS" categories of service and thus it was not possible for AFS to violate the service category customer approval requirements of the CPNI rules.

6. Further, AFS did not use, disclose to third parties, or permit access to CPNI except on an as needed basis for the provision of inside wiring installation, maintenance and repair of customer services, or to protect the rights or property of AFS, or to protect the users of AFS services and other carriers from fraudulent, abusive or unlawful use of

services, such disclosure/access not requiring customer approval. Nor did AFS engage in any marketing campaigns which utilized CPNI.

7. AFS has required all employees to sign an Employee Nondisclosure, Noncompetition and Assignment Agreement ("Agreement") as a condition of employment or continued employment. Under the terms of the Agreement AFS employees are prohibited from divulging confidential information of any customer to any individual or entity outside of AFS. This provision is binding upon employees even after their termination of employment. Furthermore, AFS employees are required to devote their full time efforts to the business of AFS and are explicitly prohibited from engaging in any other business activity that would conflict with their duties to AFS. In the event that an employee violates the Agreement AFS may terminate the employee in addition to any other remedies available at law or in equity.

8. AFS has taken, and continues to take, reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI:

a) For example, through the use of "firewalls" AFS blocked unauthorized attempts to gain access to corporate systems. In addition, via encryption of CPNI, AFS further reduced the possibility that usable CPNI data could be accessed illegally.

b) Internal access to CPNI was restricted to company employees on a "need-to-know" basis.

c) Direct customer access to CPNI was available only via a randomly-generated password provided by AFS to the customer's contact-of-record. Customer requests for replacements for lost or forgotten passwords were accepted only from the previously-established customer contact-of-record and such replacements passwords were likewise transmitted only to the contact-of-record.

d) Notification of customer account changes were accepted only from the customer contact-of-record and AFS immediately notified and acknowledged such a change to the customer via return telephone call or e-mail communication with the customer contact-of-record.

9. Although no such breaches have occurred, AFS is aware of and will comply with all requirements of 47 C.F.R. Section 64.2011 to notify the appropriate agencies and the impacted customer(s) of any security breach involving CPNI within the prescribed time frames and to maintain the appropriate records.

10. During CY2007 AFS received no complaints relating to the unauthorized release of CPNI.

CERTIFICATE OF COMPLIANCE

Pursuant to Section 64.2009(e) of the rules and regulations of the Federal Communications Commission ("FCC"), 47 C.F.R. §64.2009(e) I, Gita Ramachandran, Chief Financial Officer and agent of American Fiber Systems, Inc. ("AFS"), hereby certify that during Calendar Year 2007 AFS was in material compliance with the rules and regulations governing the use and disclosure of Customer Proprietary Network Information, 47 C.F.R. §64, Subpart U ("CPNI Rules").

The attached "Statement of CPNI Operating Procedures" constitutes a statement explaining how AFS' operating procedures generally ensured that AFS was in material compliance with the CPNI Rules during Calendar Year 2007, and is based upon the reasonable diligence of the undersigned.

Gita Ramachandran
Chief Financial Officer

Date: February 29, 2008

DOCKET FILE COPY ORIGINAL

Annual 47 C.F.R. S: 64.2009(e) CPNI Certification of Telekom Malaysia-USA, Inc. for 2007

EB Docket 06-36

Date filed: February 25, 2008

Form 499 Filer ID: 825447

Name of signatory: Mohamed Asri Jaafar

Title of signatory: General Manager

I, Mohamed Asri Jaafar, certify that I am an officer of Telekom Malaysia–USA, Inc. ("TM-USA"), and acting as an agent of TM-USA, that I have personal knowledge that TM-USA has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. S: 64.2001 et seq.

Attached to this certification is an accompanying statement explaining how TM-USA's procedures ensure that it is in compliance with the requirements set forth in section 64.2001 et seq. of the Commission's rules.

TM-USA has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

TM-USA has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed _____

No. of Copies rec'd 0+4
List ABCDE

STATEMENT REGARDING OPERATING PROCEDURES IMPLEMENTING 47 C.F.R. SUBPART U GOVERNING THE USE OF CUSTOMER PROPRIETARY NETWORK INFORMATION ("CPNI")

Telekom Malaysia-USA Inc. ("TM-USA"), has established policies and procedures to assure compliance with Part 64 of Title 47 of the Code of Federal Regulations, Subpart U – Customer Proprietary Information ("CPNI") § 64.2001et. seq. of the Commission's rules.

TM-USA operates soley as a provider of wholesale international services. TM-USA does ot provide any services to end-user customers in the United States, and TM-USA does not permit CPNI to be used in its sales and marketing efforts. Nonetheless, TM-USA has implemented the following CPNI use, notice, authentication, and security procedures to ensure compliance with the Commission's rules.

I. Notice Required For Use of CPNI

TM-USA has not provided notification to its customers and has not asked for approval to use CPNI because TM-USA does not use CPNI outside of the areas that are allowed without customer approval. TM-USA does not share customers CPNI with any joint venture partner, independent contractor or any other third party. ***In the event that at a future time TM-USA decides to use CPNI in a manner that requires customer approval, it will do so in accordance with the approval and notice requirements specified in 47 CFR §§ 64.2007-64.2008 of the Commission's rules.***

II. Safeguards on the Disclosure of Customer Proprietary Network Information.

TM-USA has procedures in place to assure that customers are properly authenticated prior to disclosing CPNI. TM-USA will properly authenticate a customer prior to disclosing CPNI as follows:

(a) In person – the customer must be personally known by the employee or the customer must provide a valid photo ID matching the customer's account information.

(b) Telephone access to CPNI. TM-USA will only disclose call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides TM-USA with a password, as described in paragraph (d) below that is not prompted by the carrier asking for readily available biographical information, or account information. If the customer does not provide a password, TM-USA will only disclose call detail information by sending it to the customer's address of record, or by calling the customer at the telephone number of record. If the customer is able to provide call detail information to TM-USA during a customer-initiated call without TM-USA's assistance, then TM-USA may discuss the call detail information provided by the customer.

(c) Online access to CPNI. TM-USA will authenticate a customer without the use of readily available biographical information, or account information, prior to allowing the customer online access to CPNI related to a telecommunications service account. Once authenticated, the customer may only obtain online access to CPNI related to a telecommunications service account through a password that is not prompted by TM-USA asking for readily available biographical information, or account information.

(d) Establishment of a Password and Back-up Authentication Methods for Lost or Forgotten Passwords. To establish a password, TM-USA must authenticate the customer without the use of readily available biographical information, or account information. TM-USA may

create a back-up customer authentication method in the event of a lost or forgotten password, but such back-up customer authentication method may not prompt the customer for readily available biographical information, or account information. If a customer cannot provide the correct password or the correct response for the back-up customer authentication method, the customer must establish a new password as described in this paragraph.

(e) Notification of account changes. TM-USA will promptly notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed. This notification may be through a voicemail or text message sent by TM-USA to the telephone number of record, or by mail to the address of record, and will not reveal the changed information or be sent to the new account information.

(f) Wholesale Customers – at this time TM-USA has no retail end user customers and only provides wholesale carrier-to-carrier services in the United States. TM-USA and its wholesale carrier customers address issues of CPNI protection specifically in their contracts, and these may or may not differ somewhat from the authentication procedures identified in paragraphs (a) through (e) above. TM-USA's wholesale customers each have a dedicated account representative.

III. Notification of Customer Proprietary Network Information Security Breaches.

In the case of a breach, TM-USA will as soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach, electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through the FCC link at http://www.fcc.gov/eb/cpni.

(a) Notify customers only after 7 full business days have passed after notification to the USSS and the FBI unless the USSS or FBI has requested an extension.

(b) If there is an extraordinarily urgent need to notify affected customers or the public sooner in order to avoid immediate and irreparable harm, it will be done only after consultation with the relevant investigating agency. TM-USA shall cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification.

(c) Maintain a record of any breaches discovered, notifications made to the USSS and the FBI and notifications made to customers. The record will include if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. TM-USA shall retain the record for a minimum of 2 years.

(d) Include a summary of the breach in the annual compliance certificate filed with the FCC.

IV. Record Retention

TM-USA shall retain all information regarding CPNI. Following are the minimum retention periods TM-USA has established:

- CPNI notification and records of approval if used – five years
- Marketing campaign if used – one year
- Breaches: five years
- Annual Certification – five years
- Employee training certification – five years
- All other information – two years.